UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,932	03/09/2004	Akio Sakamoto	6005-4-0016	3286

22434 7590 04/29/2008

BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
PHAM, MICHAEL	
ART UNIT	PAPER NUMBER
2167	
MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/796,932	SAKAMOTO ET AL.	
	Examiner	Art Unit	
	MICHAEL D. PHAM	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/15/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

Status of claims

1. Claims 1-34 are pending.

2. Claims 1-34 have been examined.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, 14, 15-20, 28, and 29-34 rejected under 35 U.S.C. 102(e) as being US Patent Application Publication 2005/0086529 by Buchsbaum (hereafter Buchsbaum).

Claim 1:

Buchsbaum discloses the following claimed limitations:

"Collecting, from the database server that manages the database, data sets maintained permanently by the database server and comprising user behavior data that indicates a first set of behavior by one or more users relative to the database, wherein the collecting includes reading, from the database server, the data sets comprising user behavior data;" [0017, gathering and maintaining knowledge of the behavior of an authorized user. Further disclosing, build and

maintain a profile of the behavior of a user and/or terminal, with respect to its operations toward databases, through tracking, or monitoring user activity within the database system. Accordingly, collecting (0017, gathering/building), from the database server that manages the database (0017, database system), data sets maintained permanently by the database server (0017, profiles) and comprise user behavior data that indicates a first set of behavior by one or more users relative to the database (0017, user behavior), wherein the collecting includes reading, from the database server (0017, within the database system), the data sets comprising user behavior data (0017, user behavior) is suggested.]

"Processing and storing one or more sets of users behavior data as historical data, said one or more sets of user behavior data including said user behavior data that indicates the first set of behavior by the one or more users relative to the database;"[0035, discloses constructing a user/terminal profile based on the raw data, collected by the listener and stored in this system database. Further disclosing, 0035, profiles are constructed initially within a 'learning period' and updated. 0017, profiles of the behavior of the user and/or terminal, with respect to operations toward databases, through tracking or monitoring, of user activity within the database system and to compare each new use of the system by the user to a known profile. Accordingly, processing and storing (0035, constructing/storing) one or more sets of users behavior data as historical data (0035, profiles constructed initially within a learning period), said one or more sets of user behavior data including said user behavior data that indicates the first set of behavior by the one or more users relative to the database (0035, profiles. 0017, profile of behavior of a user) is suggested.]

"Analyzing the historical data to determine behavior patterns;" [0035, marking any anomaly, i.e. deviation from the values stored within the profile, found in the comparison phase and grading it according to an algorithm using profile data and system owner instructions such as levels of threshold. 0019, A user's or terminal, information profile will show, after a learning period, certain consistencies in user activity toward a database. Accordingly, analyzing (0035, comparing/grading) the historical data to determine behavior patterns (0019, consistencies in user activity) is suggested.]

"Receiving, from the database server that manages the database, data sets maintained permanently by the database server and comprising a new set of user behavior data that indicates a second set of behavior by the one or more users relative to the database, the receiving includes reading, from the database server, the data sets comprising the new set of user behavior data; "[0029, discloses for example, a vacation schedule database may be utilized to flag any data activity performed by a user when the vacation schedule indicates that the user should be inactive. 0035, user profiles updated. Accordingly, receiving, from the database server that manages the database (0029, database may be utilized), data sets maintained permanently by the database server (0035, profiles) and comprising a new set of user behavior data that indicates a second set of behavior by the one or more users relative to the database (0029, data activity performed by user when the vacation schedule indicates that the user should be inactive), the receiving includes reading, from the database server, the data sets comprising the new set of user behavior data (flagging data) is suggested.]

"Performing a comparison based on the new set of user behavior data and the determined behavior patterns;"[0035, Comparing each trace of data access to the appropriate profile;

marking any deviation from the values stored within the profile found in the comparison phase and grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, performing a comparison (0035, comparing) based on the new set of user behavior data (0035, trace of data) and the determined behavior patterns (0035, profiles) is suggested.]

"Determining, based on the comparison, whether the new set of user behavior data satisfies a set of criteria;"[0035, grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, determining, based on the comparison, whether the new set of user behavior satisfies a set of criteria (levels of threshold) is suggested.]

"If the new set of user behavior data satisfies the set of criteria, then determining that the new set of user behavior data represents anomalous activity; and"[0019, cause system to flag anomalous user behavior and, when necessary, to issue an alarm that potential misuse or abuse is indicated. Accordingly, if the new set of user behavior data satisfies the set of criteria, then determining that the new set of user behavior data represents anomalous activity (0019, flag anomalous user behavior) is suggested.]

"Responding to the determination by performing a targeted operation." [0019, to issue an alarm that potential misuse or abuse is indicated. Accordingly, responding to the determination by performing a targeted operation (0019, issue an alarm) is suggested.]

Claim 2:

Buchsbaum discloses:

"Determining if the new set of user behavior data violates a rule based policy;" [0035 set of rules representing common statistics, mathematical or other techniques. 0035, comparing each data trace of data access to the appropriate profile. 0038, comparison calculated. 0039, a substantial deviation will produce a warning with appropriate grade] and

"If the new set of user behavior data violates the rule based policy, then determining that the new set of user behavior data represents anomalous activity."[0039, a substantial deviation will produce a warning with appropriate grade.]

Claim 3:

Buchsbaum discloses, "wherein collecting user behavior data comprises:

Reading information from an audit trail of a database manager" [0034, collects on continuous basis, data from the management apparatus' data files].

Claim 4:

Buchsbaum discloses ", wherein collecting user behavior data from the database server at a monitor level selected from at least one of:

Information about database access for one or more selected database objects;"

"Information about database access for one or more selected database users; and" [0034, user identification]

"Information about database access for one or more database user sessions."

Claim 5:

Buchsbaum discloses "wherein collecting user behavior data comprises:

Receiving a type of information to be monitored;" [0017, monitoring, of user activity]

"Determining a monitoring level from the type of information; and"[0026, sensitivity level]

"activating audit options of the database manager based upon the monitoring level determined."[0039, watch flag to increase the sensitivity for the next time check. A further, more detailed check might be done, to assist in analyzing behavior, deviation and improving warning accuracy. Accordingly, activating audit options of the database manager (0039, A further more detailed check might be done) based upon the monitoring level determined (0039, sensitivity) is suggested]

Claim 6:

Buchsbaum discloses, "wherein analyzing the historical data to determine behavior patterns further comprises:

Determining a statistical model from the historical data." [0023, information is gathered and comes subject to a set of operations, or algorithms, constructing variety of characteristics, statistically or other, for a specific user and/or terminal. To enhance precision, an algorithm calculating the standard deviation, or any predefined and/or acceptable deviation formula, is applied for the same or alike characteristics.]

Claim 14:

Buchsbaum discloses ", wherein performing a targeted operation comprises at least one of raising an alert; sending an email; producing a report; performing a visualization." [0019, issue alarm]

Claim 15:

Buchsbaum discloses the following claimed limitations:

"Collecting, from the database server that manages the database, data sets maintained permanently by the database server and comprising user behavior data that indicates a first set of behavior by one or more users relative to the database, wherein the collecting includes reading, from the database server, the data sets comprising user behavior data;" [0017, gathering and maintaining knowledge of the behavior of an authorized user. Further disclosing, build and maintain a profile of the behavior of a user and/or terminal, with respect to its operations toward databases, through tracking, or monitoring user activity within the database system. Accordingly, collecting (0017, gathering/building), from the database server that manages the database (0017, database system), data sets maintained permanently by the database server (0017, profiles) and comprise user behavior data that indicates a first set of behavior by one or more users relative to the database (0017, user behavior), wherein the collecting includes reading, from the database server (0017, within the database system), the data sets comprising user behavior data (0017, user behavior) is suggested.]

"Processing and storing one or more sets of users behavior data as historical data, said one or more sets of user behavior data including said user behavior data that indicates the first set

of behavior by the one or more users relative to the database;" [0035, discloses constructing a user/terminal profile based on the raw data, collected by the listener and stored in this system database. Further disclosing, 0035, profiles are constructed initially within a 'learning period' and updated. 0017, profiles of the behavior of the user and/or terminal, with respect to operations toward databases, through tracking or monitoring, of user activity within the database system and to compare each new use of the system by the user to a known profile. Accordingly, processing and storing (0035, constructing/storing) one or more sets of users behavior data as historical data (0035, profiles constructed initially within a learning period), said one or more sets of user behavior data including said user behavior data that indicates the first set of behavior by the one or more users relative to the database (0035, profiles. 0017, profile of behavior of a user) is suggested.]

"Analyzing the historical data to determine behavior patterns;" [0035, marking any anomaly, i.e. deviation from the values stored within the profile, found in the comparison phase and grading it according to an algorithm using profile data and system owner instructions such as levels of threshold. 0019, A user's or terminal, information profile will show, after a learning period, certain consistencies in user activity toward a database. Accordingly, analyzing (0035, comparing/grading) the historical data to determine behavior patterns (0019, consistencies in user activity) is suggested.]

"Receiving, from the database server that manages the database, data sets maintained permanently by the database server and comprising a new set of user behavior data that indicates

a second set of behavior by the one or more users relative to the database, the receiving includes reading, from the database server, the data sets comprising the new set of user behavior data;" [0029, discloses for example, a vacation schedule database may be utilized to flag any data activity performed by a user when the vacation schedule indicates that the user should be inactive. 0035, user profiles updated. Accordingly, receiving, from the database server that manages the database (0029, database may be utilized), data sets maintained permanently by the database server (0035, profiles) and comprising a new set of user behavior data that indicates a second set of behavior by the one or more users relative to the database (0029, data activity performed by user when the vacation schedule indicates that the user should be inactive), the receiving includes reading, from the database server, the data sets comprising the new set of user behavior data (flagging data) is suggested.]

"Performing a comparison based on the new set of user behavior data and the determined behavior patterns;" [0035, Comparing each trace of data access to the appropriate profile; marking any deviation from the values stored within the profile found in the comparison phase and grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, performing a comparison (0035, comparing) based on the new set of user behavior data (0035, trace of data) and the determined behavior patterns (0035, profiles) is suggested.]

"Determining, based on the comparison, whether the new set of user behavior data satisfies a set of criteria;" [0035, grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, determining, based on the

comparison, whether the new set of user behavior satisfies a set of criteria (levels of threshold) is suggested.]

"If the new set of user behavior data satisfies the set of criteria, then determining that the new set of user behavior data represents anomalous activity; and" [0019, cause system to flag anomalous user behavior and, when necessary, to issue an alarm that potential misuse or abuse is indicated. Accordingly, if the new set of user behavior data satisfies the set of criteria, then determining that the new set of user behavior data represents anomalous activity (0019, flag anomalous user behavior) is suggested.]

"Responding to the determination by performing a targeted operation." [0019, to issue an alarm that potential misuse or abuse is indicated. Accordingly, responding to the determination by performing a targeted operation (0019, issue an alarm) is suggested.]

Claim 16:

Buchsbaum discloses ",further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of:

Determining if the new set of user behavior data violates a rule based policy;" [0035 set of rules representing common statistics, mathematical or other techniques. 0035, comparing each data trace of data access to the appropriate profile. 0038, comparison calculated. 0039, a substantial deviation will produce a warning with appropriate grade] and

"If the new set of user behavior data violates the rule based policy, then determining that the new set of user behavior data represents anomalous activity."[0039, a substantial deviation will produce a warning with appropriate grade.]

Claim 17:

Buchsbaum discloses, "wherein the instructions for carrying out the step of collecting user behavior data comprise instructions for carrying out the step of:

Reading information from an audit trail of the database manager" [0034, collects on continuous basis, data from the management apparatus' data files].

Claim 18:

Buchsbaum discloses, "wherein the instructions for carrying out the step of collecting user behavior data further comprise instructions for carrying out the step of collecting user behavior data at a monitoring level selected from at least one of:

Information about database access for one or more selected database objects;"

"Information about database access for one or more selected database users;" [0034, user identification] and

"Information about database access for one or more selected database user sessions."

Claim 19:

Buchsbaum discloses, "wherein the instructions for carrying out the step of collecting user behavior data further comprise instructions for carrying out the steps of:

Receiving a type of information to be monitored;" [0017, monitoring, of user activity]

"Determining a monitoring level from the type of information; and"[0026, sensitivity level]

"activating audit options of the database manager based upon the monitoring level determined."[0039, watch flag to increase the sensitivity for the next time check. A further, more detailed check might be done, to assist in analyzing behavior, deviation and improving warning accuracy. Accordingly, activating audit options of the database manager (0039, A further more detailed check might be done) based upon the monitoring level determined (0039, sensitivity) is suggested]

Claim 20:

Buchsbaum discloses, "wherein the instructions for carrying out the step of analyzing the historical data to determine behavior patterns further comprise instructions for carrying out the step of:

Determining a statistical model from the historical data" [0023, information is gathered and comes subject to a set of operations, or algorithms, constructing variety of characteristics, statistically or other, for a specific user and/or terminal. To enhance precision, an algorithm calculating the standard deviation, or any predefined and/or acceptable deviation formula, is applied for the same or alike characteristics.]

Claim 28:

Buchsbaum discloses ",wherein the instructions for carrying out the step of performing a targeted operation comprises comprise instructions for carrying out at least one of: raising an alert; sending an email; producing a report; performing a visualization." [0019, issue alarm]

Claim 29:

Buchsbaum discloses the following claimed limitations:

"Means for collecting from a database server that manages a database, data sets maintained permanently by the database server that manage a database, data sets maintained permanently by the database server and comprising user behavior data that indicates a first set of behavior by one or more users relative to the database, wherein the collecting includes reading, from the database server, the data sets comprising user behavior;" [0017, gathering and maintaining knowledge of the behavior of an authorized user. Further disclosing, build and maintain a profile of the behavior of a user and/or terminal, with respect to its operations toward databases, through tracking, or monitoring user activity within the database system. Accordingly, collecting (0017, gathering/building), from the database server that manages the database (0017, database system), data sets maintained permanently by the database server (0017, profiles) and comprise user behavior data that indicates a first set of behavior by one or more users relative to the database (0017, user behavior), wherein the collecting includes reading, from the database server (0017, within the database system), the data sets comprising user behavior data (0017, user behavior) is suggested.]

"Means for processing and storing one or more sets of user behavior data as historical data, said one or more sets of user behavior data including said user behavior data indicates the first set of behavior by the one or more users relative to the database;" [0035, discloses constructing a user/terminal profile based on the raw data, collected by the listener and stored in this system database. Further disclosing, 0035, profiles are constructed initially within a 'learning period' and updated. 0017, profiles of the behavior of the user and/or terminal, with respect to operations toward databases, through tracking or monitoring, of user activity within

the database system and to compare each new use of the system by the user to a known profile. Accordingly, processing and storing (0035, constructing/storing) one or more sets of users behavior data as historical data (0035, profiles constructed initially within a learning period), said one or more sets of user behavior data including said user behavior data that indicates the first set of behavior by the one or more users relative to the database (0035, profiles. 0017, profile of behavior of a user) is suggested.]

"Means for analyzing the historical data to determine behavior patterns;" [0035, marking any anomaly, i.e. deviation from the values stored within the profile, found in the comparison phase and grading it according to an algorithm using profile data and system owner instructions such as levels of threshold. 0019, A user's or terminal, information profile will show, after a learning period, certain consistencies in user activity toward a database. Accordingly, analyzing (0035, comparing/grading) the historical data to determine behavior patterns (0019, consistencies in user activity) is suggested.]

"Means for receiving, from the database server that manages the database, data sets maintained permanently by the database server and comprising a new set of user behavior data that indicates a second set of behavior by the one or more users relative to the database, the means for receiving including means for reading, from the database server, the data sets comprising the new set of user behavior data;" [0029, discloses for example, a vacation schedule database may be utilized to flag any data activity performed by a user when the vacation schedule indicates that the user should be inactive. 0035, user profiles updated. Accordingly, receiving, from the database server that manages the database (0029, database may be utilized), data sets maintained permanently by the database server (0035, profiles) and comprising a new

set of user behavior data that indicates a second set of behavior by the one or more users relative to the database (0029, data activity performed by user when the vacation schedule indicates that the user should be inactive), the receiving includes reading, from the database server, the data sets comprising the new set of user behavior data (flagging data) is suggested.]

"Means for performing a comparison based on the new set of user behavior data and the determined behavior patterns;" [0035, Comparing each trace of data access to the appropriate profile; marking any deviation from the values stored within the profile found in the comparison phase and grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, performing a comparison (0035, comparing) based on the new set of user behavior data (0035, trace of data) and the determined behavior patterns (0035, profiles) is suggested.]

"Means for determining based on the comparison, whether the new set of user behavior data satisfies a set of criteria;" [0035, grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, determining, based on the comparison, whether the new set of user behavior satisfies a set of criteria (levels of threshold) is suggested.]

"Means for determining that the new set of user behavior data represents anomalous activity, if the new set of user behavior data satisfies the set of criteria; and" [0019, cause system to flag anomalous user behavior and, when necessary, to issue an alarm that potential misuse or abuse is indicated. Accordingly, if the new set of user behavior data satisfies the set of criteria, then determining that the new set of user behavior data represents anomalous activity (0019, flag anomalous user behavior) is suggested.]

"means for responding to the determination by performing a targeted operation." [0019, to issue an alarm that potential misuse or abuse is indicated. Accordingly, responding to the determination by performing a targeted operation (0019, issue an alarm) is suggested.]

Claim 30:

Buchsbaum discloses the following claimed limitations:

"A data collector for (a) collecting, from a database server that manages a database, data sets maintained permanently by the database server and comprising user behavior data that indicates a first set of behavior, by one or more users relative to the database, wherein the collecting includes reading, from the database server, the data sets comprising user behavior data," [0017, gathering and maintaining knowledge of the behavior of an authorized user. Further disclosing, build and maintain a profile of the behavior of a user and/or terminal, with respect to its operations toward databases, through tracking, or monitoring user activity within the database system. Accordingly, collecting (0017, gathering/building), from the database server that manages the database (0017, database system), data sets maintained permanently by the database server (0017, profiles) and comprise user behavior data that indicates a first set of behavior by one or more users relative to the database (0017, user behavior), wherein the collecting includes reading, from the database server (0017, within the database system), the data sets comprising user behavior data (0017, user behavior) is suggested.]

"(b) processing and storing the one or more sets of user behavior data as historical data, said one or more sets of user behavior data including said user behavior data that indicates the first set of behavior by the one or more users relative to the database, and" [0035, discloses

constructing a user/terminal profile based on the raw data, collected by the listener and stored in this system database. Further disclosing, 0035, profiles are constructed initially within a 'learning period' and updated. 0017, profiles of the behavior of the user and/or terminal, with respect to operations toward databases, through tracking or monitoring, of user activity within the database system and to compare each new use of the system by the user to a known profile. Accordingly, processing and storing (0035, constructing/storing) one or more sets of users behavior data as historical data (0035, profiles constructed initially within a learning period), said one or more sets of user behavior data including said user behavior data that indicates the first set of behavior by the one or more users relative to the database (0035, profiles. 0017, profile of behavior of a user) is suggested.]

"(c) receiving, from the database server that manages the database, data sets maintained permanently by the database server and comprising a new set of user behavior data that indicates a second set of behavior by the one or more users relative to the database, the receiving including reading, from the database server, the data sets comprising the new set of user behavior data;" [0029, discloses for example, a vacation schedule database may be utilized to flag any data activity performed by a user when the vacation schedule indicates that the user should be inactive. 0035, user profiles updated. Accordingly, receiving, from the database server that manages the database (0029, database may be utilized), data sets maintained permanently by the database server (0035, profiles) and comprising a new set of user behavior data that indicates a second set of behavior by the one or more users relative to the database (0029, data activity performed by user when the vacation schedule indicates that the user should be inactive), the

receiving includes reading, from the database server, the data sets comprising the new set of user behavior data (flagging data) is suggested.]

"A data analyzer for analyzing the historical data to determine behavior patterns; and" [0035, marking any anomaly, i.e. deviation from the values stored within the profile, found in the comparison phase and grading it according to an algorithm using profile data and system owner instructions such as levels of threshold. 0019, A user's or terminal, information profile will show, after a learning period, certain consistencies in user activity toward a database. Accordingly, analyzing (0035, comparing/grading) the historical data to determine behavior patterns (0019, consistencies in user activity) is suggested.]

"An anomaly detector for

(a) performing a comparison based on the new set of user behavior data and the determined behavior patterns," [0035, Comparing each trace of data access to the appropriate profile; marking any deviation from the values stored within the profile found in the comparison phase and grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, performing a comparison (0035, comparing) based on the new set of user behavior data (0035, trace of data) and the determined behavior patterns (0035, profiles) is suggested.]

"(b) determining, based on the comparison, whether the new set of user behavior data satisfies a set of criteria," [0035, grading it according to an algorithm, using profile data and system owner instructions, such as levels of threshold. Accordingly, determining, based on the comparison, whether the new set of user behavior satisfies a set of criteria (levels of threshold) is suggested.]

"(c) determining that the new set of user behavior data represents anomalous activity if the new set of user behavior data satisfies the set of criteria and" [0019, cause system to flag anomalous user behavior and, when necessary, to issue an alarm that potential misuse or abuse is indicated. Accordingly, if the new set of user behavior data satisfies the set of criteria, then determining that the new set of user behavior data represents anomalous activity (0019, flag anomalous user behavior) is suggested.]

"(d) responding to the determination by performing a targeted operation." [0019, to issue an alarm that potential misuse or abuse is indicated. Accordingly, responding to the determination by performing a targeted operation (0019, issue an alarm) is suggested.]

Claim 31:

Buchsbaum discloses a database manager as database system management apparatus in figure 1 element 12. Buchsbaum does not explicitly disclose "reading information from a dynamic performance views of"

On the other hand, Denning discloses a type of metric may be a resource measure. Where X is the quantity of resources consumed by some action during a period as specified in the resource-usage field of the audit records. Accordingly, reading information from dynamic performance views is suggested by Denning as an observation of X, where X is the quantity of resources consumed by some action during a period.

Both Buchsbaum and Denning are directed to intrusion detection systems, and are therefore within the same field of endeavor. It would have been obvious to a person of an

ordinary skill in the art at the time the invention was made to have applied Denning's disclosure as noted above to the system of Buchsbaum for the purpose of detecting denial of service where an intruder is able to monopolize a resource.

Claim 32:

Buchsbaum discloses a database manager as database system management apparatus in figure 1 element 12. Buchsbaum does not explicitly disclose "reading information from a dynamic performance views of"

On the other hand, Denning discloses a type of metric may be a resource measure. Where X is the quantity of resources consumed by some action during a period as specified in the resource-usage field of the audit records. Accordingly, reading information from dynamic performance views is suggested by Denning as an observation of X, where X is the quantity of resources consumed by some action during a period.

Both Buchsbaum and Denning are directed to intrusion detection systems, and are therefore within the same field of endeavor. It would have been obvious to a person of an ordinary skill in the art at the time the invention was made to have applied Denning's disclosure as noted above to the system of Buchsbaum for the purpose of detecting denial of service where an intruder is able to monopolize a resource.

Claim 33:

Buchsbaum discloses ", wherein the data sets maintained permanently by the database server include audit trails" [0034, collects on continuous basis, data from the management apparatus' data files]

Claim 34:

Buchsbaum discloses "wherein the data sets maintained permanently by the database server include audit trails" [0034, collects on continuous basis, data from the management apparatus' data files]

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 7-13 and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication 2005/0086529 by Buchsbaum (hereafter Buchsbaum) further in view of "An Intrusion-Detection Model" by Dorothy E. Denning (hereafter Denning).

Claim 7:

Buchsbaum discloses ", wherein determining a statistical model from the historical data further comprises:

Determining a frequency of database access from the historical data;" [0023, average quantity of database access per hour, per day, per month, per year, per specific day of week, per specific day of a month, per specific timeframe of a day, etc.]

Buchsbaum does not explicitly disclose

"Determining a probability function for frequencies of database access; and"

"Determining a cumulative probability function from the probability function."

On the other hand, Denning shows "determining a probability function for frequencies of database access" as determination if it meets a confidence interval determined by chebychev's inequality (e.g. a probability function), page 225, col. 2 line 22. Denning shows "determining a cumulative probability function from the probability function" as the mean (e.g. a cumulative probability function), page 225 col. 2 line16.

Both Buchsbaum and Denning are directed to intrusion detection systems, and are therefore within the same field of endeavor. It would have been obvious to a person of an ordinary skill in the art at the time the invention was made to have applied Denning's disclosure as noted above to the system of Buchsbaum for the purpose of improving the ability to determine whether a new observation is abnormal.

Claim 8:

Buchsbaum and Denning further disclose ", wherein performing a comparison between the new set of data and the determined behavior patterns further comprises:

Testing a hypothesis using the new set of data against the statistical model." [Denning discloses as a new observation of X of n+1 is defined to be abnormal if it falls outside a confidence interval that is d standard deviations from the mean for some parameter d. Accordingly, testing a hypothesis (abnormal if) using the new set of data (new observation X of n+1) against the statistical model (mean and standard deviation).]

Claim 9:

Buchsbaum and Denning further disclose ", wherein testing a hypothesis using the new set of data against the statistical model further comprises:

Determining a frequency of database access for the new set of data; and"[Buchsbaum, 0023, average quantity of database accesses. 0037, comparing specific access parameters with aggregative parameters.]

"Determining the threshold value from a guard criteria and a probability function parameter."[Denning, page 225 line 19, confidence interval; page 225 lines 21-24, d; and page 225 lines 17, standard deviation]

Claim 10:

Buchsbaum and Denning further disclose ", wherein testing a hypothesis using the new set of data against the statistical model pattern further comprises:

Comparing frequency of database access for the new set of data with the threshold value." [Denning, page 225 lines 18-20, a new observation X of n+1 is defined to be abnormal if it falls outside a confidence interval.]

Claim 11:

Buchsbaum and Denning further disclose ", wherein the historical information is about database access for one or more selected database objects and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of:

Object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location." [Buchsbaum, 0023, average quantity of database access per hour]

Claim 12:

Buchsbaum and Denning further disclose "wherein the historical information is about database access for one or more selected database users, and wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of:

User access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination

of at least two of operating system user, database user, and location." [Buchsbaum, 0023, average quantity of database access per hour]

Claim 13:

Buchsbaum and Denning further disclose ", wherein the historical information is about database access for one or more selected database user sessions wherein determining a frequency of database access from the historical data further comprises determining a frequency of at least one of:

Number of page reads per session, access duration per session, number of page reads per unit time." [Buchsbaum, 0023, average quantity of database access per hour]

Claim 21:

Buchsbaum discloses ",wherein the instructions for carrying out the step of determining a statistical model from the historical data further comprise instructions for carrying out the step of:

Determining a frequency of database access from the historical data;" [0023, average quantity of database access per hour, per day, per month, per year, per specific day of week, per specific day of a month, per specific timeframe of a day, etc.]

Buchsbaum does not explicitly disclose

"Determining a probability function for frequencies of database access; and"

"Determining a cumulative probability function from the probability function."

On the other hand, Denning shows "determining a probability function for frequencies of database access" as determination if it meets a confidence interval determined by chebychev's inequality (e.g. a probability function), page 225, col. 2 line 22. Denning shows "determining a cumulative probability function from the probability function" as the mean (e.g. a cumulative probability function), page 225 col. 2 line16.

Both Buchsbaum and Denning are directed to intrusion detection systems, and are therefore within the same field of endeavor. It would have been obvious to a person of an ordinary skill in the art at the time the invention was made to have applied Denning's disclosure as noted above to the system of Buchsbaum for the purpose of improving the ability to determine whether a new observation is abnormal.

Claim 22:

Buchsbaum and Denning further disclose ",wherein the instructions for carrying out the step of performing a comparison between the new set of data and the determined behavior patterns further comprise instructions for carrying out the step of:

Testing a hypothesis using the new set of data against the statistical model." [Denning discloses as a new observation of X of n+1 is defined to be abnormal if it falls outside a confidence interval that is d standard deviations from the mean for some parameter d. Accordingly, testing a hypothesis (abnormal if) using the new set of data (new observation X of n+1) against the statistical model (mean and standard deviation).]

Claim 23:

Buchsbaum and Denning further disclose "wherein the instructions for carrying out the step of testing a hypothesis using the new set of data against the statistical model further comprising instructions for carrying out the steps of:

Determining a frequency of database access for the new set of data; and"[Buchsbaum, 0023, average quantity of database accesses. 0037, comparing specific access parameters with aggregative parameters.]

"Determining the threshold value from a guard criteria and a probability function parameter."[Denning, page 225 line 19, confidence interval; page 225 lines 21-24, d; and page 225 lines 17, standard deviation]

Claim 24:

Buchsbaum and Denning further disclose ",wherein the instructions for carrying out the step of testing a hypothesis using the new set of data against the statistical model further comprise instructions for carrying out the step of:

Comparing frequency of database access for the new set of data with the threshold value." [Denning, page 225 lines 18-20, a new observation X of n+1 is defined to be abnormal if it falls outside a confidence interval.]

Claim 25:

Buchsbaum and Denning further disclose ",wherein the historical information is about database access for one or more selected database objects and wherein the instructions for carrying out the step of determining a frequency of database access from the historical data further comprise instructions for carrying out the step of determining a frequency of at least one of:

Object access frequency by hour of day, object access frequency by hour of day and operating system user, object access frequency by hour of day and database user, object access frequency by hour of day and location, object access frequency by hour of day and combination of at least two of operating system user, database user and location." [Buchsbaum, 0023, average quantity of database access per hour]

Claim 26:

Buchsbaum and Denning further disclose "wherein the historical information is about database access for one or more selected database users and wherein the instructions for carrying out the step of determining a frequency of database access from the historical data further comprise instructions for carrying out the step of determining a frequency of at least one of:

User access frequency by hour of day, user access frequency by hour of day and operating system user, user access frequency by hour of day and database user, user access frequency by hour of day and location, user access frequency by hour of day and a combination of at least two of operating system user, database user, and location." [Buchsbaum, 0023, average quantity of database access per hour]

Claim 27:

Buchsbaum and Denning further disclose ",wherein the historical information is about database access for one or more selected database user sessions and wherein the instructions for carrying out the step of determining a frequency of database access from the historical data further comprise instructions for carrying out the step of determining a frequency of at least one of:

Number of page reads per session, access duration per session, number of page reads per unit time." [Buchsbaum, 0023, average quantity of database access per hour]

Response to Arguments

7. Applicant's arguments filed 2/4/08 have been fully considered but they are not persuasive. Applicant's assert the following (lettered):

A. A declaration of prior invention under 37 CFR 1.131, removes the prior art reference.

In response, it appears Applicants are relying on reduction to practice prior to the effective date of the reference.

From MPEP 715.07:

> The essential thing to be shown under 37 CFR 1.131 is priority of invention and this may be done by any satisfactory evidence of the fact. FACTS, not conclusions, must be alleged. Evidence in the form of exhibits may accompany the affidavit or declaration. **Each exhibit relied upon should be specifically referred to in the affidavit or declaration, in terms of what it is relied upon to show.**
>
> A general allegation that the invention was completed prior to the date of the reference is not sufficient. *Ex parte Saunders*, 1883 C.D. 23, 23 O.G. 1224 (Comm'r Pat. 1883). Similarly, a declaration by the inventor to the effect that his or her invention was conceived or reduced to practice prior to the reference date, **without a statement of facts demonstrating the correctness of this conclusion, is insufficient to satisfy 37 CFR 1.131.**
>
> When reviewing a 37 CFR 1.131 affidavit or declaration, the examiner must consider all of the evidence presented in its entirety, including the affidavits or declarations and all accompanying exhibits, records and "notes." **An accompanying exhibit need not**

support all claimed limitations, provided that any missing limitation is supported by the declaration itself. *Ex parte Ovshinsky*, 10 USPQ2d 1075 (Bd. Pat. App. & Inter. 1989).

The affidavit or declaration and exhibits must clearly explain which facts or data applicant is relying on to show completion of his or her invention prior to the particular date. **Vague and general statements in broad terms about what the exhibits describe along with a general assertion that the exhibits describe a reduction to practice "amounts essentially to mere pleading, unsupported by proof or a showing of facts"** and, thus, does not satisfy the requirements of 37 CFR 1.131(b). *In re Borkowski*, 505 F.2d 713, 184 USPQ 29 (CCPA 1974). **Applicant must give a clear explanation of the exhibits pointing out exactly what facts are established and relied on by applicant.** 505 F.2d at 718-19, 184 USPQ at 33. See also *In re Harry,* 333 F.2d 920, 142 USPQ 164 (CCPA 1964) (Affidavit "asserts that facts exist but does not tell what they are or when they occurred.").

According to the record there is no exhibit relied upon. There exists only an affidavit stating that the invention was built and tested prior to the date of the reference. However, there are no facts demonstrating the correctness of this conclusion. There are no facts that support, the limitations of the claims. Applicants did not give a clear explanation pointing out **exactly** what facts are established and relied upon from the affidavit and/or exhibits with respect to the claim limitations.

Conclusion

8. The prior art made of record listed on PTO-892 and not relied, if any, upon is considered pertinent to applicant's disclosure.

Contact Information

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael D. Pham whose telephone number is (571)272-3924. The examiner can normally be reached on Monday - Friday 9am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/M. D. P./
Michael Pham
Art Unit 2167
Examiner

John Cottingham
Art Unit 2167
Supervisor

/John R. Cottingham/

Supervisory Patent Examiner, Art Unit 2167